Published and Copyright (c) 1999 - 2016
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1836 09/09/16

~ Get Shamed by Chrome! ~ People Are Talking! ~ Laptop Pioneer Dies!
~ Researcher Gets Prison ~ Video Games Get A Day! ~ Firebee News Update!
~ PlayStation Now for PC ~ Programmer Arrested! ~ PlayStation 4 Pro!

~ USBee Steals Your Data ~ MacOS Sierra Out Soon! ~ USB Kill Stick!

-* Facebook Restores Napalm Girl *-
-* OPM Failed To Detect The 2nd Hacker *-
-* Duke Nukem 3D 20th Anniversary Edition Tour *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Well, the long Labor Day weekend has come and gone, fairly quietly, I might add. The weather here wasn't all that great; and I worked most of the weekend. So, we really didn't do much in the way of the typical "end of summer" celebration. There's always this weekend to have a barbecue or two, so really no big deal!

The presidential campaigns are heating up (again, still?) with the two major party candidates continuing to hammer at each other. No big surprises in that regard! We'll just have to keep tuned in to the news and see what kind of interesting things each of them does to keep us entertained. This is proving to be one of the most strangest (I can't think of the best adjective to fit!) presidential elections that I can remember!

Until next time...

=~=~=~=

FireBee News Update

By Fred Horvat

Last submission I discussed that I brought the FireBee to work to test out EasyMiNT on the work network because I was having DNS issues at home. The FireBee ran EasyMiNT perfectly at work which obviously left me puzzled. So I brought the FireBee back home to try it out again and it did not work at home like before. Differences between home and work are the higher speed Internet connection and high priced network equipment. So next step was to start eliminating extra networking equipment between the FireBee and the Internet at home. Piece by piece I cut out hubs and switches until I was down to my Cable Modem connected to my WiFi Router. This still did not solve the issue. I went and checked my router settings as to who s DNS I was using. The ISPs (my ISP is Time Warner) or another DNS like Google s or Open DNS. My router was configured to use Google s DNS. The DNS settings on my router were IPV4 settings of 8.8.8.8 which is Google. Generally Time Warner s DNS is fine but on occasion in the past I had issues so I

manually set my router a couple of years ago to Google DNS. OK this is what I wanted and it still didn t work.

The next step was to replace my router. All I had for spares was a couple of really old B and B+G routers from about 10 years ago. A coworker had a TP-Link router with a fresh load of DD-WRT software on it. http://www.dd-wrt.com/site/index   DD-WRT is open source and highly regarded WiFi Router software. My coworker gave me the router to take home and test the FireBee with it. I connect the TP-Link router to my Cable Modem and then the FireBee to the router and turned everything on. The TP-Link worked fine with the standard FireBee FreeMiNT but with EasyMiNT I still had the same DNS issues.

So now what? I started testing other things at home like Pinging (see if an address is reachable) Web Sites and doing Trace Routes (seeing the route across the Internet from me to the Site). So I did something simple like PINGing my router via its IP address. Strange thing was that it took about 60 seconds or more before the PING would start processing. It appeared frozen but once it contacted the router it would respond every second like normal. Just that it would take 60 plus seconds to start working. TRACEROUTE tp a Website would sit for about 30-60 seconds and time out.

At this point I decided to bring the FireBee back to work. I set it all up and connected it to the network and everything worked fine again! I tried the PING command to a server on the network and it responded immediately. I tried a TRACEROUTE to a Web Site in this case IBM.COM and it worked. Everything worked as expected.

So I brought the FireBee back home, hooked it all up and same problems as before. Since I narrowed my network down to just the FireBee as the only device on the network there is not anything interfering with the FireBee. I also tried another router (DD-WRT firmware) that I assume would be a better working router than what I am currently using. This leaves me down to the Cable Modem or ISP (Time Warner) that the issue lies with. I have an older DOCSIS 2.0 Cable Modem. This may be the issue. A current DOCSIS 3.0 Cable Modem may solve the issue. I have very poor Internet Speed where I live so a DOCSIS 2.0 cable modem is still faster than what my speeds will ever be. But a DOCSIS 3.0 cable modem handles the connection much better than the older DOCSIS 2.0 modem does.

So that is where I am at with my DNS issues and EasyMiNT on the FireBee. If I find a solution or make other changes I will report my findings in a future submission.

Until Next Time

=~=~=~=

->In This Week’s Gaming Section - Sony PlayStation 4 Pro Coming!
  """""""""""""""""""""""""""""""   PlayStation Now for PC Available!

Video Games Finally Get Their Day!
And more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

Sony PlayStation 4 Pro Coming November 10

Sony s planning a one-two punch this holiday season to take the wind out of Microsoft s sails. The company on Wednesday unveiled a pair of new PlayStation 4 consoles, both of which will be out this holiday season.

A slimmer version of the PlayStation 4 will hit the market next week Sept. 14 for $299, replacing the existing PS4 model. And on Nov. 10, the PlayStation 4 Pro a high-end console that focuses squarely on 4K and high-dynamic range (HDR) video, will go on sale for $399.

Neither was exactly a surprise. Word of the PS4 Slim (which will just be called PlayStation 4) leaked weeks ago and everything from an unboxing video to a review of the system has already run, despite Sony s previous refusal to officially acknowledge its existence. And Sony confirmed the existence of the high-end model, then code-named Neo, back in June.

But each system serves a purpose in the company s fight with Microsoft for dominance in the gaming world.

The PS4 Slim comes a month after Microsoft began shipping the Xbox One S, a slim version of its flagship console. Sony has held a commanding lead in hardware sales this generation and a refresh of the current hardware at the same time as its competition could help ensure it stays in the lead. (The PS4 has sold more than 40 million units worldwide an estimated 2:1 margin over the Xbox One, according to estimates from Electronic Arts earlier this year.)

We know there are still a large number of gamers waiting to join the PlayStation 4 family, said Andrew House, president and group CEO of Sony Interactive Entertainment. [The slimmer PS4] will appeal to a wider audience who are looking to buy the best entertainment system for their home.

Things get a bit more interesting with PlayStation 4 Pro, though. The high-end system is designed to appeal to hardcore gamers and videophiles. Sony hammered its belief in 4K TV and HDR technology, with lead architect Mark Cerny calling HDR the most exciting advance in TV technology in the past decade . The enhanced graphics chip in the PS4 Pro will also make experiences in the upcoming PlayStation VR smoother, Sony said.

Not only will future games such as Spider Man, Watch Dogs 2 and Mass Effect 4 Andromeda be built around both systems, but several older titles, including Uncharted 4, will receive patches to improve their graphical quality when played on a PS4 Pro.

Additionally, Sony said, Netflix and YouTube will offer 4K apps for high-quality video streaming. And to help push HDR adoption forward, a firmware upgrade will go out next week to all existing PS4 units making them HDR (but not 4K) capable.

TVs with both 4K and HDR are still far from common in people s homes, though. To make the PS4 Pro appealing to those users, Sony noted that the system can detect the type of TV it s hooked up to. Developers can then use that power to enhance graphics on a standard HDTV by increasing the frame rate and other tricks.

Microsoft s high-end system, code-named Project Scorpio, was announced in June, but isn t due until holiday 2017. Microsoft will likely point out that Sony failed to offer any hard tech specs for the PS4 Pro in its presentation. At E3, Microsoft officials unveiled a laundry list of impressive processing power, including eight CPU cores and six teraflops of GPU power.

 We believe it will be the most powerful console ever built, said Phil Spencer, head of Microsoft s Xbox division, during the console s introduction.

Sony, though, has the timing advantage in releasing this year.

 We realized that the highly discriminating gamer, there is always a desire for advancement and they want it this generation, said House. [So] we re adjusting and accelerating our innovation cadence.

While it s easy to think of both Scorpio and PlayStation 4 Pro as next generation upgrades, that s not exactly right (though it s not entirely wrong, either).

As the gaming world has evolved, so has the definition of next generation systems. Rather than hitting reset and launching entirely new consoles, both companies are offering systems that play all existing games for the PS4 and Xbox One, but greatly enhance the hardware power.

It s not unlike the world of PC gaming, where systems aren t reinvented, they re simply upgraded.

Despite that, Sony attempted to argue that the PS4 Pro doesn t represent a new generation of consoles.

 PlayStation 4 Pro is not intended to blur the lines between console generations, said Cerny.

Analysts, though, say it s really a matter of semantics.

 The traditional console cycle is dead, said P.J. McNealy, CEO and Founder, Digital World Research.

PlayStation Now for PC Available in the US & Canada

Sony Interactive Entertainment announced today that PlayStation Now for PC is now available in the United States and Canada. To start streaming the over 400 PlayStation 3 games on your Windows PC you ll need to download the app and have a DualShock 4, a PlayStation Network account, current PS Now subscription or 7-Day Free Trial (credit card required), and a 5Mbps or greater internet connection.

If you want to go wireless with your DualShock 4 when using PS Now on PC, Sony says the DualShock 4 USB Wireless Adaptor will be available in North America beginning on September 6 for $24.99.

In other PlayStation Now news, the September 2016 PlayStation Now additions in the US and Canada include these six titles:

Borderlands: Ultimate Edition
Heavy Rain + The Taxidermist DLC
Mafia II
Ni no Kuni: Wrath of the White Witch
Sid Meier s Civilization Revolution
Tomb Raider Game of the Year Edition

In October, one of the games being added in the second annual Shocktober celebration will be Castlevania: Harmony of Despair.

Finally, if you re looking to sign up for PlayStation Now or want to extend your subscription, Sony is offering a 12-month subscription for $99.99 USD/CAN, which is a discount of more than 55% over the regular monthly subscription price. The 12-month subscription is only available for a limited time, but we have not announced the end date for the promotion, Sony s James Martin added.

Duke Nukem 3D 20th Anniversary Edition World Tour Coming to Playstation 4 Xbox One and Windows

When you think of classic first person shooters you will probably fondly remember potty mouthed Duke Nukem 3D. 3D Realms were in a unique position as they were fighting not only a plethora of competition - some of that competition was Doom, Doom II and other popular first person shooters of the time. How do you take on competition like that? You go in another direction. Rather than go all surreal and otherworldly with their story and setting, 3D Realms went more realistic with Duke Nukem 3D. Well, as realistic as you can when you have jetpack flying giant humanized pigs in police uniforms.

When I first moved out to Texas to join the Duke Nukem 3D development team in the mid-nineties, I could not possibly predict that we were all going to be part of the emergence of the 3D First Person videogame genre that would ultimately impact the entire videogame industry, said Randy Pitchford, President of

Gearbox Software. Making it possible for Allen, Richard, Lee and Jon to all come back together 20 years later to bring a whole new episode to the classic game is just one of those rare and incredible things that I hope will bring joy and happiness to hardcore videogame fans new and old.

Duke Nukem 3D 20th Anniversary Edition World Tour is scheduled to hit the Sony Playstation 4, Xbox One and Windows PC s via Steam. This is not just a straight port of an old game, no, they are doing some work on this one and improving it.

Hail to the King, Baby episode is all new and original. Contains eight levels that were created by the original designers Allen Blum III and Richard Levelord Gray.

Come Get Some features all new music by composer Lee Jackson who was the original composer of Grabbag, an iconic theme from the original game. Also additional voice work by John St. John - Duke himself, is added.

I ve Got Balls of Steel is a behind the scenes tell all with the development team.

I m Looking Good! lets players enjoy the game using the original 1996 graphics set. You will also be able to toggle in real time over to the new graphics using the True3D Rendering technology.

Grab Duke Nukem 3D 20th Anniversary Edition World Tour on Playstation 4, Xbox One and Windows via Steam on October 11th.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Video Games Finally Get Their Day

Grab your joysticks, Monday is National Video Games Day.

And, yes, it s a big deal.

Last year the video game industry generated $23.5 billion domestically that s more than the movie ($11 billion) and music ($7 billion) industries combined in the United States.

Worldwide the video game industry is estimated to generate nearly $100 billion this year.

And this global phenomenon all started with ...

Tic-Tac-Toe.

In 1952, A.S. Douglas programmed the Tic-Tac-Toe game OXO (aka

Noughts and Crosses) on an Electronic Delay Storage Automatic Calculator, or EDSAC basically, a large, expensive, and, by today s standards, quite primitive computer as part of his PhD dissertation at the University of Cambridge. The rudimentary game was displayed on a small, oval dot matrix CRT monitor with a player using a telephone s rotary dial to select movements against the computer opponent.

Then in 1958 in Upton, N.Y., a Brookhaven National Laboratories physicist named Willy Higinbotham invented Tennis for Two, a two-player tennis-like game displayed on an oscilloscope.

OXO and Tennis for Two were warm-ups to the first major breakthrough for video games: Spacewar.

Programmed in 1961 by MIT student Steve Russell along with help from classmates Spacewar was a two-player contest played on an expensive car-sized lab computer. Largely considered the first video game, Spacewar featured dueling spaceships that could rotate left and right, thrust forward, and fire torpedoes, and later hyperspace to another spot on the screen a button combination still in use by current games. There was also a sun that exerted real-time gravity to affect the ships.

As Spacewar grew in popularity beyond MIT, a college student in Utah named Nolan Bushnell was so impressed by the game that he later programmed his own knock-off, Computer Space, in the 1960s. Computer Space eventually became the first coin-operated video game in 1971, and while it flopped, the game s commercial failure spurred Bushnell to start his own company a year later: Atari.

The entrepreneur would have much better success with Atari s first arcade game, Pong; the first test unit, placed in a dive bar in Sunnyvale, Calif., in September, 1972, actually broke because it was filled with too many quarters.

As with Computer Space, Bushnell s idea for Pong wasn t original. Months before Pong was released, he saw a demonstration of a table tennis game on the first home video game system, the Magnavox Odyssey, which was designed by Ralph Baer whom many consider to be the true father of video games in the late 1960s.

Atari and Home Pong, a consumer version of its arcade hit, would later compete against the Magnavox Odyssey. The Odyssey lost that battle, as did the Odyssey 2 video game console against the Atari 2600 several years later.

Exhaustively covered by the informative and entertaining The Ultimate History of Video Games by Steven L. Kent, the early years of the video game industry is an enthralling soap opera of double and even triple-dealing; cocaine and prostitutes; lawsuits; the brilliant rise of start-ups to billion-dollar titans and their spectacular fall into ignominy and financial ruin. And more lawsuits.

It s a wonder how the industry survived it almost didn t let alone that it grew into such dominance and popularity.

In that respect, Monday and the National Video Games Day before

then are not just about playing video games, but celebrating an industry whose day has finally come.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

GOP Report: OPM Failed To Detect 2nd Hacker in Breach

As the U.S. Office of Personnel Management purged a hacker, another intruder who secretly infiltrated the system stole 20.5 million records containing personal information of government workers and contractors, many with top security clearances, according to a new GOP Congressional report.

Republican members of the House Oversight and Government Reform Committee on Sept. 7 released the 241-page report about the 2014-2015 breach. It contends OPM leaders could have prevented the theft of personal information of tens of millions of individuals.

"The longstanding failure of OPM's leadership to implement basic cyber hygiene - such as maintaining current authorities to operate and employing strong multifactor authentication, despite years of warning from the inspector general - represents a failure of culture and leadership, not technology," states the report, written under the direction of Committee Chairman Jason Chaffetz, R-Utah.

OPM's acting director disputes many aspects of the report and says it fails to acknowledge the many data security steps that the office has taken since the incident. Meanwhile, Democrats on the Congressional panel claim the GOP report reaches conclusions that are contrary to facts found during the committee's investigation.

The new report says that OPM was monitoring an intruder, labeled Hacker X1 when, on May 7, 2014, another hacker, Hacker X2, posed as an employee of OPM contractor KeyPoint, which conducted background investigations on prospective employees and contractors. Hacker X2, using the contractor's OPM credentials, logged into the OPM system, installed malware and created a backdoor to the network, according to the report.

Intelligence agencies had asked OPM not to kick Hacker X1 off the network so they could monitor its movements and collect intelligence on the intruder, the report notes. But when the agency noticed Hacker 1 got dangerously close to the security clearance background information, OPM - working with the Department of Homeland Security - developed a remediation plan called "the Big Bang." The government purged Hacker 1 from the system in May 2014. Still, Hacker 2 wasn't detected and remained in the OPM system post-Big Bang, according to the report. Two

months later, Hacker 2 began to exfiltrate security clearance background investigation files. In December 2014, the hacker stole personnel records; a month later, the cyber-assailant exfiltrated fingerprint data.

Basic Controls and Cutting-Edge Tools

"Had OPM implemented basic, required security controls and more expeditiously deployed cutting-edge security tools when they first learned hackers were targeting such sensitive data, they could have significantly delayed, potentially prevented or significantly mitigated the theft," the GOP report says.

The report identifies one of those controls as two-factor authentication, which, if implemented, might have prevented the breaches by both hackers.

One of the "cutting-edge" tools cited in the report is Cylance's Protect advance threat protection product, which OPM deployed after purging Hacker 1. The tool "lit up like a Christmas tree" when implemented, according to the report.

"Could they have done better? Absolutely," Cylance founder and CEO Stuart McClure said in an interview with the Associated Press. "But once they had been definitively convinced there was a breach, they took it very seriously."

OPM's Leader Responds

In a blog, OPM Acting Director Beth Cobert says she disagrees with many aspects of the report, but she did not address the specifics regarding the two hackers in her response. Cobert says the committee's report fails to fully reflect where the agency stands today in regards to IT security.

Cobert lists a number of steps OPM has taken since the breach to secure sensitive data. "The cybersecurity incidents at OPM provided a catalyst for accelerated change within our organization," she says. "Throughout this agency, management has embraced cybersecurity as a top priority."

Also critical of the Republican members' report were the committee's Democratic members, who issued a 21-page memorandum responding to the majority's account of the breach. The ranking member of the committee, Rep. Elijah Cummings, D-Md., says the Republican report reaches conclusions that are contrary to facts found during the committee's investigation. "The committee's year-long investigation into the data breaches showed that no one from the intelligence community or anywhere else detected the presence of the attackers and that these cyber spies were caught only with cutting-edge tools that OPM had deployed," Cummings says.

Cummings criticizes the Republicans for not adequately addressing contractors' role in federal cybersecurity, saying one of the most significant deficiencies uncovered during the committee's investigation was the finding that cyber requirements for government contractors are inadequate.

Through a spokesman, Federal CIO Tony Scott declined to comment on the Republican report, referring questions to OPM. In a speech last week at the National Institute of Standards and Technology,

the CIO said the way the federal government funds IT projects served as a major contributor to the OPM breach because Congress, for the most part, fails to provide adequate money to modernize agencies' IT (see US CIO: Federal Funding Process Played Key Role in OPM Hack). Newer systems, he says, are less prone to cyberattacks.

"What you have is a recipe for high costs, cost overruns, projects that can't be completed or are difficult to start and the whole litany of things that we all know historically have been true," Scott said. "And, indeed, in OPM we found exactly that."

Researcher Gets 20 Days in Prison for Hacking State Websites As Political Stunt

An anonymous reader writes from a report via Softpedia:

David Levin, 31, of Estero, Florida will spend 20 days in prison after hacking two websites belonging to the Florida state elections department. Levin, a security researcher, tested the security of two Florida state election websites without permission, and then recorded a video and posted on YouTube. The problem is that the man appearing in the video next to Levin was a candidate for the role of state election supervisor, running for the same position against the incumbent Supervisor of Elections, Sharon Harrington. Harrington reported the video to authorities, who didn't appreciate the media stunt pulled by the two, and charged the security researcher with three counts of hacking-related charges. The researcher turned himself in in May and pleaded guilty to all charges. This week, he received a 20-day prison sentence and two years of probation. In court he admitted to the whole incident being a political stunt.

Programmer Arrested for Hacking Linux Kernel Organization

A South Florida-based computer programmer made an appearance in the Southern District of Florida yesterday after being arrested Sunday on charges of hacking into computers operated by the Linux Kernel Organization and the Linux Foundation.

The Linux Kernel Organization operates the www.kernel.org website from which it distributes the Linux kernel software. The Linux Foundation is a separate nonprofit foundation that supports the www.kernel.org website.

Donald Ryan Austin, 27, of El Portal, Fla., was arrested during a traffic stop on August 28, 2016, by officers of the Miami Shores Police Department. Austin was arrested pursuant to a four-count indictment returned by a federal grand jury in the Northern District of California on June 23, 2016, and unsealed Tuesday.

Austin is charged with causing damage to four servers located in the Bay Area by installing malicious software. Specifically, he

is alleged to have gained unauthorized access to the four servers by using the credentials of an individual associated with the Linux Kernel Organization. According to the indictment, Austin used that access to install rootkit and trojan software, as well as to make other changes to the servers. Austin is charged with four counts of intentional transmission causing damage to a protected computer.

Austin made his initial appearance in federal court in Miami, on August 29, 2016. He was released on bond. His next scheduled appearance is in San Francisco at 9:30 a.m. on September 21, 2016, before the Honorable Sallie Kim, United States Magistrate Judge.

If convicted, he faces a maximum sentence of ten years of imprisonment, and a fine of $250,000, plus restitution, for each violation.

Facebook Restores Censored Nude Napalm Girl Photo Due to Historical Importance

Facebook has backtracked on its decision to censor a Norwegian journalist and newspaper s posts, reinstating the nude photo of a child fleeing napalm during the Vietnam war. Facebook had originally told The Guardian that We try to find the right balance between enabling people to express themselves while maintaining a safe and respectful experience for our global community.

Now Facebook s statement to TechCrunch (emphasis ours) is that:

> After hearing from our community, we looked again at how our Community Standards were applied in this case. An image of a naked child would normally be presumed to violate our Community Standards, and in some countries might even qualify as child pornography. In this case, we recognize the history and global importance of this image in documenting a particular moment in time. Because of its status as an iconic image of historical importance, the value of permitting sharing outweighs the value of protecting the community by removal, so we have decided to reinstate the image on Facebook where we are aware it has been removed. We will also adjust our review mechanisms to permit sharing of the image going forward. It will take some time to adjust these systems but the photo should be available for sharing in the coming days. We are always looking to improve our policies to make sure they both promote free expression and keep our community safe, and we will be engaging with publishers and other members of our global community on these important questions going forward.

Facebook continues to find itself in problematic situations as it attempts to control what appears in the News Feed. Earlier this year it cited a technical glitch for why a Live video of Philando Castile dying after being shot by police disappeared from the social network for several hours before reappearing.

At the time, Mark Zuckerberg said The images we ve seen this

week are graphic and heartbreaking, and they shine a light on the fear that millions of members of our community live with every day. That indicated that Facebook saw value in transmitting graphic and potentially disturbing content if it had news value. The company later clarified its policy to me, explaining that it only removes graphic content if it celebrates or glorifies violence.

I ve recommended that Facebook allow people to report content as graphic but newsworthy so the social network can obscure potentially offensive imagery with a warning that people can click through if they still want to view it. Right now, users can only report content as offensive or graphic, but without the caveat that they think it should stay up. Facebook says people should simply report offensive imagery and it will make the call about what to do with it.

Putting a disclaimer interstitial covering the image would have been a better option in the case of the napalm girl photo, at least until it could decide whether to simply leave it full visible, instead of deleting the posts containing it.

These censorship blunders combined with the decreasing visibility of news outlets in the feed are surely pushing publishers to reconsider their reliance on Facebook. Unfortunately, most pull too much traffic from Facebook to simply ditch it. Meanwhile, many have already began working with its Instant Articles program that decreases load time in exchange for giving Facebook sweeping control over the visual form of articles and limits the monetization, subscription, and recirculation options publishers typically use on their own sites.

In hindsight, publishers should have been working to deepen direct relationships with their readers rather than jumping head first into a channel they don t control.

Unmodified USB Devices Allow Data Theft From Air-Gapped Systems

Researchers have demonstrated how an unmodified USB device can be turned into a radio frequency (RF) transmitter and leveraged to exfiltrate potentially sensitive data from air-gapped computers.

In the past years, experts from the Cyber Security Research Center at Ben-Gurion University of the Negev in Israel analyzed methods for exfiltrating data using cellular frequencies, noise from fans and hard drives, electromagnetic signals from graphics cards, and heat emitted by the CPU and GPU.

Now they have come up with a new method that involves an unmodified USB device and an experimental piece of malware dubbed USBee.

Using USB devices to exfiltrate data from secure systems over RF is not unheard of. NSA documents leaked in 2013 showed that the agency s toolset included such capabilities. Inspired by the NSA, white hat hackers later created a hardware implant with similar

capabilities. However, these tools rely on modified USB connectors, whereas researchers have found a way to exfiltrate data using unmodified devices.

USBee is designed to leverage the USB data bus to create electromagnetic emissions from a connected device. The malware can modulate binary data over the electromagnetic waves and send it to a nearby receiver.

Experts determined that sending a sequence of 0 bits to a USB device, such as a flash drive or an external hard drive, generates electromagnetic radiation. By intentionally sending a certain sequence of 0 bits from the targeted computer to the connected USB device, the malware can generate electromagnetic radiation at specific frequencies, which can represent either a 1 bit or a 0 bit.

The data can then be captured by a nearby receiver. In their experiments, researchers used a $30 RTL-SDR software-defined radio connected to a laptop and managed to transfer data at rates of up to 80 bytes per second. This is a fairly high transfer rate that can allow the malware to transfer strong passwords and encryption keys within seconds.

The data can be transferred over a considerable distance.

Researchers have proposed several countermeasures, such as banning electronic equipment near sensitive computers, using antiviruses and intrusion detection systems, and shielding components to prevent electromagnetic emissions. However, experts noted that these methods might not always be very efficient or feasible. For instance, in the case of intrusion detection systems set up to detect certain patterns, they could result in a high rate of false positives.

Now You Can Buy USB Kill That Could Fry Your PC via USB

The manufacturer USBKill.com has commercialized USB Kill 2.0, a USB dongle that is able to fry any computer through the USB ports.

The Hong Kong-based technology manufacturer USBKill.com has created a USB dongle that is able to fry any computer into which it s plugged by using an electrical discharge. The attack is simple, the USBKill use to charge capacitors from the USB power supply, and then discharges 200 volts DC over the host device.

The designer of the USBKill presented a prototype last year, the USB device was able to destroy a laptop in a few seconds. Now they have presented the USB kill 2.0, a final release that is commercialized by USBKILL.com team.

Our tests reveal that more than 95% of all devices using USB ports will be damaged permanently or completely destroyed by a USB power surge attack . explained the researchers behind the project that explained they created the USB kill 2.0 for testing purposes. The unique device that passed the tests is the latest

version of Apple s MacBook, which uses surge-protected USB ports.

The company warns it has been designed and tested to be safe, , it is a high-voltage device it is not a toy and is only intended for responsible adults.

Hardware developers could use the USB device to evaluate the resilience of their machine against such kind of devastating power surge attacks and to prevent data theft via juice jacking.

Any public facing USB port should be considered an attack vector. In data security, these ports are often locked down to prevent exfiltration of data, or infiltration of malware, but are very often unprotected against electrical attack! reads the press release.

When the USB Kill stick is plugged in, it rapidly charges its capacitors from the USB power supply, and then discharges all in the matter of seconds, the company said in a news release.

The Juice jacking is a cyber attack where wherein malware might be installed on to, or data surreptitiously copied from, a mobile device or other computer device using a charging port that doubles as a data connection.

The USB Kill 2.0 could cause serious damage to the host, despite it isn t designed to wipe data depending on the hardware configuration it could have this effect by destroying drive controllers.

When tested on computers, the device is not designed or intended to erase data. However, depending on the hardware configuration (SSD vs platter HDD), the drive controllers may be damaged to the point that data retrieval is impractical, the company said in its marketing material.

USB Kill also said the device was created for use by hardware designers of public machines, such as photo booths, copy machines, airline entertainment systems and ticket terminals anything with exposed USB ports that need to ensure that their systems resist electrical attacks.

Finally, the general public, or anyone who wants to test or kill their own devices should equip themselves, the company stated. Penetration testers and security auditors should include the USB Kill 2.0 to their arsenal of testing tools.

The technology manufacturer USBKill.com also offer for sale a USB Protection Shield specifically designed to allow the testing of the USB Killer without damaging the host machine.

The USB Kill 2.0 stick costs around $56, meanwhile the Test Shield will go for about $15.70.

Unencrypted Website? Expect To Start Being Shamed by Google Chrome

Too many websites are being lax with the security of your passwords and credit card information, and Google says enough is enough.

The problem is this. When you visit a website that asks you to enter your password or payment card details you want to feel confident not only that the website itself is taking care with how it might store that information, but also whether the information is being sent securely from your computer or mobile phone s web browser to the site itself.

Because if that information isn t being sent in a secure fashion between your device and the website, a malicious hacker could potentially intercept the data as it is being sent and grab your login password. Perhaps the most well known risk is if you happen to be using a public Wi-Fi hotspot and you can never be quite sure if that guy sitting in the corner is trying to sniff other people s unencrypted data out of the air.

The good news is that more and more websites have jumped on board the HTTPS web encryption bandwagon, and users will have noticed the green padlock appearing in their browser s address bar to indicate a secure, encrypted connection.

If you don t see padlock icon in your address bar then you should not enter any type of sensitive information (passwords, bank account information, social security numbers, credit card numbers etc.), because of the risk of eavesdropping.

But wouldn t it be great if even more sites adopted HTTPS to properly protect our information?

Google certainly thinks so, and has announced that from January 2017 its Chrome browser will be marking HTTP sites that transmit passwords or credit cards as non-secure .

The problem up until now is that Chrome hasn t been explicitly pointing out that you re on an HTTP webpage:

> Chrome currently indicates HTTP connections with a neutral indicator. This doesn t reflect the true lack of security for HTTP connections. When you load a website over HTTP, someone else on the network can look at or modify the site before it gets to you.
>
> Studies show that users do not perceive the lack of a secure icon as a warning, but also that users become blind to warnings that occur too frequently.

In the future, Google plans to extend its HTTP warnings to cover more scenarios   its ultimate aim to label all HTTP pages as non-secure, and change the HTTP security indicator to the red triangle that we use for broken HTTPS.

Of course if Google were to take that step straight away users would be seeing a *lot* of warnings. It s a good thing that they re not rushing to extend the HTTP warning quite so far just yet, as you can imagine how many users would react. That would be a big mistake on Google s part.

But I wonder if Google is making another mistake in its approach

here.

In its warning it says Not secure . That s not really the right terminology. What they really mean is Not encrypted.

After all, it s perfectly possible to have a website that is using HTTPS web encryption and providing security correctly at that level, but is lacking security in other ways.

It would be a mistake, for instance, to find ourselves back in the bad old days when some users believed that the mere existence of a padlock in the browser bar meant that the site could be trusted and considered legitimate, when it was perfectly possible for criminals to set up a website with HTTPS if they wished or compromise a legitimate website that was using web encryption properly.

Maybe I m shouting into the wind, as educating the public about these semantic differences is surely an impossible task. But let s not hope that users make the mistake of thing that sites which don t have the Not secure warning are magically safe to use.

That grumble aside, I am in favour of anything which delivers a more encrypted web to the world. Maybe this change in Chrome will make more websites wake up to the importance of switching to HTTPS, especially on those webpages where they asking for sensitive information.

MacOS Sierra Gets A Release Date

Apple kept the focus on its mobile products during its September 2016 product event today, introducing the iPhone 7, iPhone 7 Plus and the Apple Watch Series 2. Mac computers went unmentioned during the event, but the MacO Sierra page on Apple’s site was updated to include a release date for the operating system: September 20.

As with past OS X releases, MacOS Sierra will be a free upgrade made available via the Mac’s App Store, but you will need a Mac from late-2009 or later to make the jump. Here is the list of supported Macs for MacOS Sierra:

- MacBook -- late 2009 and later
- MacBook Air -- 2010 and later
- MacBook Pro -- 2010 and later
- iMac -- late 2009 and later
- Mac Mini -- 2010 and later
- Mac Pro -- 2010 and later

Among the new features coming to MacOS Sierra are Siri integration, optimized storage via iCloud Drive, a universal clipboard, auto unlock via Apple Watch and Apple Pay on the Web.

The only Mac-related news to come out of Apple’s product event on Wednesday was that iWork will soon offer real-time collaboration.

RIP John Ellenby, Godfather of the Modern Laptop

John Ellenby managed the development of the Alto II before starting the company that built the world's first successful "clamshell" laptop. Slashdot reader fragMasterFlash quotes the New York Times:

Ellenby, a British-born computer engineer who played a critical role in paving the way for the laptop computer, died on August 17 in San Francisco. He was 75... Mr. Ellenby's pioneering work came to fruition in the early 1980s, after he founded Grid Systems, a company in Mountain View, California. As chief executive, he assembled an engineering and design team that included the noted British-born industrial designer William Moggridge.

The team produced a clamshell computer with an orange electroluminescent flat-panel display that was introduced as the Compass. It went to market in 1982. The Compass is now widely acknowledged to have been far ahead of its time.

Back in the 1980s, NASA used them as backup navigational devices on the space shuttle - one was recovered from the wreckage of the Space Shuttle Challenger - and John Poindexter, America's national security advisor during the Reagan administration, described them as "built like an armored tank". Data storage cost $8,150 - equivalent to $20,325 today.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.